

May 16, 1996

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

MAY 16 1996

In the Matter of

Implementation of Local Competition
Provisions of the Telecommunications
Act of 1996

)
)
)
)
)

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

CC Docket No. 96-98

DOCKET FILE COPY ORIGINAL

COMMENTS OF THE SECRETARY OF DEFENSE

Rebecca S. Weeks, Lt Col, USAF
Staff Judge Advocate

Carl Wayne Smith
Chief Regulatory Counsel,
Telecommunications, DOD

Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204

No. of Copies rec'd
List ABCDE

0 + 12

SUMMARY

The United States needs reliable, robust communications networks to further the goals of national defense. Therefore, DOD strongly urges the Commission to give fundamental consideration to network reliability and risk of harm to the network in implementing the provisions for interconnection and access found in the Telecommunications Act of 1996.

The Commission has an independent duty, based on its role in furthering the national defense and public safety, to ensure that interconnection and access will not create unreasonable risk to network reliability or substantially increase the possibility of harm to the network.

Increased inter-connectivity and adequate security and reliability are not mutually exclusive. The Commission can achieve an appropriate balance between these objectives and should carefully consider comments on how best to achieve this balance as they move to implement the Telecommunications Act of 1996.

Department of Defense

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

May 16, 1996
RECEIVED

MAY 16 1996
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

In the Matter of)
)
Implementation of Local Competition) CC Docket No. 96-98
Provisions of the Telecommunications)
Act of 1996)

COMMENTS OF THE SECRETARY OF DEFENSE

The Secretary of Defense, for the Department of Defense and as Executive Agent of the National Communications System¹, through duly authorized counsel, pursuant to Section 201 of the Federal Property

Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions", April 3, 1984, (49 Fed. Reg. 13471, 1984), established the National Communications System (NCS), which consists of an administrative structure involving the Executive Agent, Committee of Principals, Manager, and the telecommunications assets of the Federal organizations which are represented on the Committee of Principals. Section 1(e) of Executive Order 12472 designates the Secretary of Defense as Executive Agent of the NCS. By direction of the Executive Office of the President, the NCS member organizations (which are represented on the Committee of Principals) are: Department of Agriculture, Central Intelligence Agency, Department of Commerce, Department of Defense, Department of Energy, Federal Emergency Management Agency, General Services Administration, Department of Justice, National Aeronautics and Space Administration, the Joint Staff, Department of State, Department of Transportation, Department of Treasury, U.S. Information Agency, the Department of Veterans Affairs, Department of Health and Human Services, Department of the Interior, National Security Agency, the National Telecommunications and Information Administration and the Nuclear Regulatory Commission. The Federal Communications Commission, the United States Postal Service and the Federal Reserve Board also participate in the activities of the NCS. The vast majority of the telecommunications assets of these 23 organizations are leased from commercial communications carriers and serve the National Security and Emergency Preparedness (NS/EP) needs of the Federal government as well as State and local governments.

and Administrative Services Act of 1949, 40 U.S.C. Section 481, and the Memorandum of Understanding between the Department of Defense and the General Services Administration dated November 27, 1950, hereby files these comments in response to the Commission's Notice of Proposed Rulemaking, FCC 96-182, released April 19, 1996.²

I. Introduction

DOD fully supports "the development of a procompetitive deregulatory national policy framework for the United States." Notwithstanding support of this policy, we have some serious concerns about the impact further deregulation and unbundling of telecommunications networks may have on the security and reliability of those networks.

DOD, and other agencies of the Federal government, rely on the public switched network for many critical telecommunications services. By Executive Order 12472 dated 3 April 1984, the President directed the NCS to "seek to ensure that a national telecommunications infrastructure is developed which incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to

²DOD fully supports the comments of the General Services Administration filed separately herein by counsel for GSA.

obtain to the maximum extent practicable, the survivability of national security and emergency preparedness in all circumstances, including conditions of crisis or emergency."

Whether responding to national emergency or crisis or addressing more routine concerns, we must have a network that always works and always works well.

Section 1 of the Communications Act of 1934 established that the FCC was created in part "for the purposes of the national defense" and "for the purpose of protecting safety of life and property." 47 U.S.C. Section 151. Since the enactment of that provision, the Commission has consistently recognized its duty to consider national security and emergency preparedness concerns and goals when exercising its regulatory responsibilities. See, for example, The Consolidated Application of AT&T Company and the Specified Bell System Companies, 98 FCC 2d 141 (1983), National Security Emergency Preparedness Telecommunications Services Priority System, 3 F.C.C. Rec. 6650 (1988), MTS-WATS Market Structure Inquiry, 73 FCC 2d 222 (1979). Nothing in the Telecommunications Act of 1996 abrogates or changes FCC responsibility with regard to incorporating national defense and public safety, and more particularly national security and

emergency preparedness, concerns into the regulatory process.

II. Provisions of Section 251

At paragraph 56 of the Notice of Proposed Rulemaking, the Commission seeks comment on whether a risk to network reliability or other harm to the network should be considered in determining whether interconnection at a particular point is technically feasible. DOD urges the Commission to answer that question with an emphatic yes. We believe that risks to network reliability and harm to the network should **absolutely** be considered in determining whether interconnection at a particular point is technically feasible. The United States needs reliable, robust communications networks to further the goals of national defense and public and safety.

Risk of reduced reliability and harm to the network should also be considered as a part of the regulatory decision making process associated with collocation (paragraphs 66 through 73 of the Notice of Proposed Rulemaking) and access to network elements (paragraphs 86 through 91 of the Notice of Proposed Rulemaking).

Security and reliability concerns exist across the broad spectrum of services, facilities and equipment. However, interconnection and access to some types of facilities and

equipment may bring more risk of harm to the network than others. As one example, access to database and signaling systems, such as the SS7 system, might give someone the opportunity to cause inadvertent or malicious damage to large parts of the public switched network.

The Telecommunications Act of 1996 will allow a variety of companies to enter the telecommunications market at all levels. Additionally the Act calls for continuing deregulation of telecommunications services and providers when such deregulation is in the public interest. The goals of the 1996 Act are to increase competition, lower prices and bring new products and services to the nation. Unfortunately , a byproduct of this increased openness in the telecommunications market may be an enhanced ability by malicious parties, such as computer hackers or terrorist groups, to adversely affect the public switched network, if security is not a primary consideration. Accordingly, DOD urges the Commission to adopt interconnection rules that provide as much protection as possible against access by such parties and to carefully include security considerations in future rulemakings.

III. Role of the Commission

We believe that the Commission has an independent duty, based on the foregoing discussion of its role in furthering the national defense and public safety, to ensure that interconnection at a particular point will not create unreasonable risk to network reliability or substantially increase the possibility of harm to the network. For that reason we respectfully disagree with the Commission's tentative conclusion that such risks only be evaluated if a party alleges such harm and provides detailed information to support it. Network security and reliability should be fundamental criteria in any Commission decision on interconnection regardless of whether such harm is alleged by a party to the proceeding.

DOD recognizes that opening telecommunications networks to increased interconnection also increases the possibility of harm to the network. However, we do not believe that increased interconnectivity and adequate security are mutually exclusive. The Commission can achieve an appropriate balance between these two objectives and should consider all comments on how best to achieve this balance as it moves to implement the interconnection

May 16, 1996

provisions of the Telecommunications Act of 1996.³

The Commission has addressed security and reliability issues in a variety of dockets in the past, including In the Matter of Intelligent Networks, Docket 91-346. DOD urges the Commission to continue to give such issues careful consideration and attention in this and all future rulemakings on interconnection and access.

Respectfully submitted,



Rebecca S. Weeks, Lt Col, USAF
Staff Judge Advocate
(703) 607-6096



Carl Wayne Smith
Chief Regulatory Counsel,
Telecommunications, DoD

Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204

³The Network Reliability Council could provide useful recommendations on some of these issues.